Safeguard Computer Security Evaluation Matrix (SCSEM)

Cisco IOS

Release IV

December 3, 2008
Version 0.5

Internal Revenue Service

Tester: *Insert Tester Name*
Date: *Insert Date(s) Testing Occurred*
Location: *Insert Location testing was conducted*
Agency POC(s): *Insert Agency interviewee(s) names*

Test ID	**NIST ID**	Test Objective	Test Steps	Expected Results	Actual Results	Pass / Fail	**Comments/Supporting Evidence**
1	AU-8, SC-13	Ensure the lifetime of a Message Digest 5 (MD5) Key expiration is set to never expire. The lifetime of the MD5 key should be configured as infinite for route authentication, if supported by the current approved router software version. NOTE: Only Enhanced Interior Gateway Routing Protocol (EIGRP), and Routing Information Protocol (RIP) Version 2 use key chains.	1. Review the running configuration to determine if key authentication has been defined with an infinite lifetime. NOTE: When using MD5 authentication keys, it is imperative the site is in compliance with the Network Time Protocol (NTP) policies. *Example Technical Checks:* --- *Procedures:* *1. Type 'sh run | inc enable secret' in an enable console window:* *2. Type 'sh run | inc enable password' in an enable console window:* *Expected Results:* *1. Something similar to the following line should appear:* *enable secret 5 1yPL1$zNGeZu9blpdYLYEobTNwX* *2.No line should appear that starts with " enable password".* *Note: The 'enable password' command is included with the Cisco IOS for backward compatibility with older versions of the IOS. The newer "enable secret" command uses an MD5 hash for encryption of the privileged level password, and should be used in its place.*	MD5 Key lifetime should be set to "infinite".			

Test ID	**NIST ID**	Test Objective	Test Steps	Expected Results	Actual Results	Pass / Fail	**Comments/Supporting Evidence**
2	IA-2	Ensure that when an authentication server is used for administrative access to the router, only one account is defined locally on the router for use in an emergency (i.e., authentication server or connection to the server is down).	1. Review the running configuration and verify that only one local account has been defined. An example of a local account is shown in the example below: Username xxxxxxx password 7 xxxxxxxxxxxx	Only one local account should be defined on the router when an authentication server is used.			
3	IA-3	An approval process is in place for granting access to routers operated under TACACS.	Procedures: 1. Acquire from the agency personnel documents containing the following information: - A list of users that will require access to all telecomm equipment. - The list of specified devices that users require access to. - The list of access level required for the users for specified devices. - Proof of local manager approval for stated access to routers under their - authority. - The list of authorized approving managers 2. Verify that the information in the documentation is the same as the actual list of TACACS accounts and access privileges.	A documented process exists for approving account access to routers operated under TACACS			
4	AC-5, IA-1, IA-2, IA-3, IA-4	Ensure each user has their own account to access the router with username and password.	1. Review router configurations for local accounts defined to router. If an authentication server is being used, examine those accounts with access to the routers.	Individual user accounts should be created for each authorized router administrator. Groups, user accounts without passwords, or duplicate accounts should not exist.			

Test ID	**NIST ID**	Test Objective	Test Steps	Expected Results	Actual Results	Pass / Fail	**Comments/Supporting Evidence**
5	AC-8	Checks to see if a warning banner is displayed before a successful logon.	Procedures: Run the command 'show config' and verify that the configuration file includes a command beginning with 'set banner motd' that contains an appropriate warning banner. Expected Results: The contents of the banner should consist of something similar to the following. ---------- This system may contain Government information, which is restricted to authorized users ONLY. Unauthorized access, use, misuse, or modification of this computer system or of the data contained herein or in transit to/from this system constitutes a violation of Title 18, United States Code, Section 1030, and may subject the individual to Criminal and Civil penalties pursuant to Title 26, United States Code, Sections 7213, 7213A (the Taxpayer Browsing Protection Act), and 7431. This system and equipment are subject to monitoring to ensure proper performance of applicable security features or procedures. Such monitoring may result in the acquisition, recording and analysis of all data being communicated, transmitted, processed or stored in this system by a user. If monitoring re	A warning banner is displayed before a successful logon.			
6	IA-3	TACACS user IDs must follow username standards whenever possible.	Procedures: 1. Verify that the router is utilizing TACACS as the authentication method by executing the 'show tacacs' command. 2. Discuss with the security administrator to ensure that the password policy is followed for tacacs users.	All user id's, including TACACS user id's follow approved username standards			

Test ID	**NIST ID**	Test Objective	Test Steps	Expected Results	Actual Results	Pass / Fail	**Comments/Supporting Evidence**
7	IA-2	Password complexity, aging and history are properly enforced.	Procedures: Verify that the authentication server's configuration parameters meet the following requirements: a) Minimum password length of 8 characters b) Passwords must contain at least one number or special character, and a combination of at least one lower and uppercase letter. c) Maximum password age of 60 days for priviledged user and 90 days fro standard user accounts. d) Minimum password age of 15 days e) Password history for the previous 6 passwords f) Prohibit the use of a username within a password g) Prohibit the use of dictionary words or common passwords h) Prohibit the use of words from a customized list of dictionary words and common passwords i) Administrators can override minimum password age limits when changing passwords j) Users are forced to change their initial password during their first logon	Password strength and complexity requirements are met.			

Test ID	**NIST ID**	Test Objective	Test Steps	Expected Results	Actual Results	Pass / Fail	**Comments/Supporting Evidence**
8	AC-6, IA-3	The router administrator will ensure that all user accounts are assigned the lowest privilege level that allows them to perform their duties.	1. There are sixteen (16) possible privilege levels that can be specified for users in the router configuration. The levels can map to commands, which have set privilege levels—or you can reassign levels to commands. Usernames with corresponding passwords can be set to a specific level. There would be several username, name and password, password followed by username name privilege level. The user will automatically be granted that privilege level upon logging in. The following is an example of assigning a privilege level to a local user account and changing the default privilege levels of the configure terminal command: *Username junior-engineer1 privilege 7 password xxxxxx* *Username senior-engineer1 privilege 15 password xxxxxxx* *Privilege exec level 7 configure terminal*	Each user should have access to only the privileges they require to perform their respective duties. Access to the highest privilege levels should be restricted to a few users.			
9	AC-2	Ensure accounts that are no longer required are immediately removed from the authentication server or router.	1. Verify that the site is in compliance by reviewing site's responsibilities list. 2. Reconcile site's responsibilities list with those accounts defined locally or in the authentication server. 3. For each authentication method in use, confirm that there is a process in place to identify unused accounts and disable or delete them after 90 days.	Procedures should be in place to enforce proper account administration. Accounts that are no longer needed should be disabled or removed immediately from the system.			

Test ID	**NIST ID**	Test Objective	Test Steps	Expected Results	Actual Results	Pass / Fail	**Comments/Supporting Evidence**
10	AC-2, IA-2	Ensure the enabled secret password does not match any other username password, enabled password, or any other enabled secret password.	Interview the router's administrator(s) to see if this is being enforced on all Cisco routers. Check for the following: Ensure that the enable secret password is a unique password constructed using a length of 8 characters and a combination of at least 1 numeric or special character, 1 lowercase and 1 uppercase letter, and that it does not contain versions of the router ID or location ID. Note: The router ID can be identified by executing the 'show config | include hostname' command.	Each router should be configured with a unique enabled secret password and remove all others.			
11	IA-3, IA-5	Ensure passwords are not visible when displaying the router configuration. Type 5 encryption should be used for the enable mode password (i.e., enable secret password).	Examine all Cisco router configurations to determine if the global command service password-encryption is present.	The router administrator will configure each router using the service password encryption option. Service password-encryption is the required global config mode command.			

Test ID	**NIST ID**	Test Objective	Test Steps	Expected Results	Actual Results	Pass / Fail	**Comments/Supporting Evidence**
12	AC-3, IA-2, SC-8, SC-9	Ensure route management utilizes the Out-Of-Band (OOB) or direct connection methods for communication device management.	Interview the ISSO to determine if the site is compliant with this requirement. Example technical checks for access control: ---------- *1. Type the following command from an enable console window: 'show running-config'. Examine the subsections for "line con 0", "line aux 0", and "line vty 0 4". Each subsection should have a password assigned, which should be encrypted, and should have a line that begins with "login <authentication method>" where <authentication method> is either "local" (for local authentication) or "tacacs", "radius", or "kerberos" (if a centralized authentication server is used for authentication).* *2. If remote access is being used for administration of the router, check that access control lists are in place to restrict which IP addresses are allowed access to the router. Type the following command: show access-lists. Make a note of the numbering of the access-lists, and then type the following command: 'show running-config'. Look for the subsection for the VTY terminals – "line vty 0 4". Note: There should be a line within the con*	OOB or direct connection method should be implemented with authenticated access control, strong two-factor authentication, encryption of the management session, and audit logs when OOB management is necessary.			

Test ID	**NIST ID**	Test Objective	Test Steps	Expected Results	Actual Results	Pass / Fail	**Comments/Supporting Evidence**
13	AC-3, IA-2, SC-8, SC-9, SC-13, SC-23	Ensure the proper authorized network administrator is the only one who can access the device by ensuring Out-Of-Band (OOB) access enforces the following security restriction: -Two-factor authentication (e.g., Secure ID, PKI) - Encryption of management session (Federal Information Processing Standard (FIPS) 140-2 validated encryption) - Auditing	1. Review router configuration to ensure that an authentication server is being used. 2. Review router configuration to verify that a two-factor authentication method is implemented.	Router should be configured to utilize the most current supported version of Secure Shell (SSH) with all security patches applied. Router should be configured to ensure authenticated access control, strong two-factor authentication, encryption of the management session, and audit logs are all being incorporated in the access scheme.			
14	AC-3, IA-2	Ensure that all Out-Of-Band (OOB) management connections to the router require passwords.	1. Review each router's configuration to ensure that the console port and the vty ports used by the Out-Of-Band Management (OOBM) network require a login prompt. *The configuration should look similar to the following:* *line con 0* *login authentication admin_only* *exec-timeout 10 0* *line vty 0 4* *login authentication admin_only* *exec-timeout 0* *transport input ssh*	OOB management connections to the router should have passwords.			

Test ID	**NIST ID**	Test Objective	Test Steps	Expected Results	Actual Results	Pass / Fail	**Comments/Supporting Evidence**
15	AC-10, AC-11, CM-4	Ensure the router console port is configured to timeout after 10 minutes or less of inactivity.	1. Review each Cisco router configuration to ensure that the console is disabled after 10 minutes of inactivity. The configuration should look similar to the following: line con 0 login authentication admin_only exec-timeout 10 0	Timeout for unattended console port is set for no longer than 10 minutes via the exec-timeout command.			
16	AC-3	Ensure modems are not connected to the console or auxiliary ports.	1. Physically inspect any local routers to ensure modems are not connected.	Modems should not be connected to the console or auxiliary ports.			
17	AC-3	Ensure that the router's auxiliary port is disabled.	1. View each Cisco router's configuration to ensure that the auxiliary port is disabled with a configuration similar to the following: line aux 0 no exec transport input none	Auxiliary ports should be disabled on all routers.			
18	AC2, AC-17, IA-5	Ensure use of in-band management is limited to situations where the use of Out-Of-Band (OOB) management would hinder operational commitments or when emergency situations arise. Use of in-band management should be approved on a case-by-case documented basis.	1. Interview the ISSO for compliance. 2. Request documentation.	OOB management should be primarily used and in-band management should have limited use.			

Test ID	**NIST ID**	Test Objective	Test Steps	Expected Results	Actual Results	Pass / Fail	**Comments/Supporting Evidence**
19	AC-2, AC-17, IA-5, SC-13	Ensure that all in-band management connections to the router require passwords.	1. Review each Cisco router's configuration to ensure that the Virtual Teletype Terminal (VTY) ports require a login prompt. The configuration should similar to the following: line vty 0 4 login authentication admin_only exec-timeout 10 0 transport input ssh	All in-band management connections to the router require passwords.			
20	AC-2, AC-17, IA-5, SC-8, SC-9, SC-13, SC-23	Ensure the proper authorized network administrator is the only one who can access the device by ensuring in-band access enforces the following security restrictions: -Two-factor authentication (e.g., Secure ID, IRS PKI) -Encryption of management session (Federal Information Processing Standard (FIPS) 140-2 validated encryption) -Auditing -Two-factor authentication discussion	1. Review the router configuration to ensure that an authentication server is being used. 2. Review the router configuration to verify that a two-factor authentication method has been implemented.	The router should utilize the most current supported version of Secure Shell (SSH) with all security patches applied. Routers should be configured to ensure authenticated access control, strong two-factor authentication, encryption of the management session, and audit logs are all being incorporated in the access scheme.			

Test ID	**NIST ID**	Test Objective	Test Steps	Expected Results	Actual Results	Pass / Fail	**Comments/Supporting Evidence**
21	AC-4, AC-17	Ensure that the router only allows in-band management sessions from authorized Internet Protocol (IP) addresses from the internal network.	1. Review all router configurations and verify that only authorized internal connections are allowed on Virtual Teletype Terminal (VTY) ports. The configuration should look similar to the following: access-list 3 permit 192.168.1.10 log access-list 3 permit 192.168.1.11 log access-list 3 deny any . line vty 0 4 access-class 3 in	Router only allows in-band management sessions from authorized IP address within the internal network.			
22	AC-1. AC-17, SC-8, SC-9, SC-13, SC-23	Ensure in-band management access to the router is secured using Federal Information Processing Standard (FIPS) 140-2 validated encryption such as Advanced Encryption System (AES), Triple Data Encryption Standard (3DES), Secure Shell (SSH), or Secure Sockets Layer (SSL).	1. Review all Cisco router configurations and verify that only SSH is allowed on the Virtual Teletype Terminal (VTY) ports. The configuration should look similar to the following: line vty 0 4 transport input ssh	SSH connections are allowed to access VTY ports.			
23	SC-10	Ensure Secure Shell (SSH) timeout value is set to 60 seconds or less, causing incomplete SSH connections to shut down after 60 seconds or less.	1. Review the global configuration or execute show ssh to verify the timeout is set for 60 seconds or less. The default is 120 seconds. The configuration should look similar to the following: Ip ssh time-out 60	SSH session timeout is set to 60 seconds or less.			
24	AC-7	Ensure the maximum number of unsuccessful Secure Shell (SSH) login attempts is set to three (3), locking access to the router.	1. Review the global configuration or execute the show ssh command to verify the authentication retry is set for 3. The configuration should look similar to the following: ip ssh authentication-retries 3	Maximum number of unsuccessful SSH login attempts is set to three (3).			

Test ID	**NIST ID**	Test Objective	Test Steps	Expected Results	Actual Results	Pass / Fail	**Comments/Supporting Evidence**
25	AC-7, AC-12, SC-10	Ensure the timeout for in-band management access is set for no longer than ten (10) minutes.	1. Review each router's configuration to ensure that the Virtual Teletype Terminal (VTY) ports are disabled about 10 minutes of inactivity. The configuration should look similar to the following: line vty 0 4 login authentication admin_only exec-timeout 10 0 transport input ssh	In-band management access is set for no longer than 10 minutes.			
26	AU-2	Ensure the Access Control List (ACL) that is bound to the Virtual Teletype Terminal (VTY) ports is configured to log permitted and denied access attempts.	1. Review each router configuration to ensure that all connection attempts to the VTY ports are logged. The configuration should look similar to the following: access-list 3 permit tcp host x.x.x.x any eq 23 log access-list 3 deny any log . line vty 0 4 access-class 3 in	Permitted and denied access attempts to the VTY ports are logged.			

Test ID	**NIST ID**	Test Objective	Test Steps	Expected Results	Actual Results	Pass / Fail	**Comments/Supporting Evidence**
27	SI-2	Ensure that the latest stable Operating System (OS) is implemented on each router in accordance with the current Network Infrastructure Security Checklist.	1. Cisco IOS - execute the show version to verify installed IOS version is at 12.3 or later. Procedures From an enable console window, type 'show version'. Note: Newer releases of the Cisco IOS are in general more secure, more stable, and offers greater features than older releases. It is recommended to never be more than one or two releases out of date. The IOS should not be older than version 12.x. It should also be "Release" version software, and not an "Early Deployment" or "Maintenance Interim" release. Release versions of the Cisco IOS are the most stable version of the IOS available and have undergone thorough testing for production.	Latest operating systems in accordance with Network Infrastructure Security Checklist should be implemented.			
28	AC-10	Ensure Transmission Control Protocol (TCP) Keep-Alives for Telnet Session are enabled.	1. Review all Cisco router configurations to verify that tcp-keepalives-in are enabled.	TCP Keep-Alives for Telnet Session are enabled.			
29	CM-6	Ensure configuration auto-loading is disabled.	1. Review all Cisco router configurations to verify that the commands boot network and service config are not included. NOTE: Disabled by default in version 12.0, will not be displayed in the running configuration.	Configuration auto-loading is disabled.			

Test ID	**NIST ID**	Test Objective	Test Steps	Expected Results	Actual Results	Pass / Fail	**Comments/Supporting Evidence**
30	CM-7	All unnecessary services on the router are disabled.	Procedures: 1. Type 'sh run | inc small-servers' from an enable console window (There should be no response, indicating that both tcp-small-servers and udp-small-servers have not been enabled). 2. Type 'sh run' from an enable console window. Confirm that the following lines exist for each interface (or as a global command, if indicated below): - no ip redirects - no ip proxy-arp - no ip gratuitous-arps - no cdp enable - no mop enable - no ip unreachables - no ip ident - no ip source-route (found in a global command; not under an interface) - no ip bootp server (found in a global command; not under an interface) - no service pad (found in a global command; not under an interface) - no service dhcp (found in a global command; not under an interface) - no ip classless (found in a global command; not under an interface) - no ip http server (found in a global command; not under an interface) - no ftp-server enable -no ip rcmd rcp-enable -no ip rcmd rsh-enable	All unnecessary services on the router are disabled.			
31	AC-3	Ensure Internet Protocol (IP) directed broadcast is disabled on all router interfaces.	1. For Cisco IOS version 12.0 and higher, review the running configuration to verify that it does not contain the command ip directed-broadcast. For versions prior to 12.0, ensure the command no ip directed-broadcast is displayed in the running configuration.	IP directed broadcasts are disabled.			

Test ID	NIST ID	Test Objective	Test Steps	Expected Results	Actual Results	Pass / Fail	Comments/Supporting Evidence
32	AU-8	Ensure that an approved authoritative time server is used.	Procedures: 1. Type 'sh run | inc ntp server' from an enable console window to see if NTP is configured. The response should show: 2. To verify that the NTP client has been configured for authentication, run the 'sh run' command and look for lines in the configuration similar to the following: ntp server <ip.address> ntp authentication-key 10 md5 1043100A0014000E180F2F32 7 ntp authenticate ntp trusted-key 10	The router uses the NTP service to synchronize its time with an IRS approved authoritative time server.			
33	CM-7	Ensure Simple Network Management Protocol (SNMP) is blocked at all external interfaces.	Procedures: 1. Type 'show snmp' to verify SNMP has been enabled (if not,skip the remainder procedures). If snmp v3 is being used, type 'sh run | inc snmp' from an enable prompt window and review the authprivgroup setting. The last parameter should be set to Priv, which provides authentication and encryption. "Auth" means authentication but no enncryption, while "Noauth" means that no encryption or authentication is used. 2. Evaluate the strength of the community name strings. The "snmp community" settings contain hard-to-guess community names 3. Determine if unencrypted read/write access is possible. 4. Confirm router access is restricted by access control lists. The numbers at the end of the lines refer to ACL numbers for either read only (RO) or read/write (RW) access. Similar ACL entries: 5. If SNMP read/write access is permitted, review the permit/deny statements associated by typing 'sh access-lists'. A line similar to the following appears in one of the ACL's: 6. Type 'sh snmp | inc logging' from an enable console window. The router should NOT respo snmp-server group authprivgroup v3 priv	Expected Results: 1. snmp-server group authprivgroup v3 priv 3. Unencrypted read-write access should not be possible. Read-write access should not be enabled when snmp v1 or v2 is in use. Read-write access should only be enabled for snmp v3 when the priv authprivgroup mode is in use. 4. snmp-server community password6 RO 6 snmp-server community password8 RW 8 5. snmp-server tftp-server-list 98 6. SNMP logging: disabled			

Test ID	**NIST ID**	Test Objective	Test Steps	Expected Results	Actual Results	Pass / Fail	**Comments/Supporting Evidence**
34	CM-7	Ensure Simple Network Management Protocol (SNMP) is only enabled in the read mode; Read/Write is not enabled unless approved and documented by the ISSO .	1. Review all router configurations to ensure SNMP access from the network management stations is read only. The configuration look similar to the following: access-list 10 permit host x.x.x.x snmp-server community xxxxxxx ro 10	SNMP is enabled in the read-only mode.			
35	SC-5	Ensure a maximum wait interval for establishing a Transmission Control Protocol (TCP) connection request to the router is set to 10 seconds or less, or implement a feature to rate-limit TCP SYN traffic destined to the router.	1. Cisco – Review the router configuration to ensure the ip tcp synwait-time command is in place to monitor TCP connection requests to the router. The configuration should look similar to the following: ip tcp synwait-time 10	A maximum wait interval for establishing a TCP connection request to the router is set to ten (10) seconds or less.			
36	SC-5	Ensure Cisco Express Forwarding (CEF) is enabled to improve router stability during a SYN flood attack to the network.	1. Cisco – Review all Cisco router configurations to ensure that CEF has been enabled. The configuration should look similar to the following: ip cef CAVEAT: If the site has implemented SYN flood protection for the network using the perimeter firewall, there is not an additional requirement to implement it on the router.	CEF has been enabled.			

Test ID	**NIST ID**	Test Objective	Test Steps	Expected Results	Actual Results	Pass / Fail	**Comments/Supporting Evidence**
37	AU-3	Ensure all routers are configured to log severity levels zero (0) through six (6) and send log data to a syslog server.	1. Review all router configurations to ensure that all routers log messages for severity levels 0 through 6. By specifying informational, all severity levels will be included. For Cisco routers, a sample configuration would look similar to the following: logging on logging host x.x.x.x logging console critical logging trap informational logging facility buildingA	All routers are configured to log severity levels zero (0) through six (6) and send log data to a syslog server.			
38	AC-3	Ensure, when saving and loading configurations, the running and startup configurations are synchronized.	1. Cisco – Compare the startup and running configurations. This can be done by using the show running-config command and show startup-config.	Running and start-up configurations are synchronized.			
39	AC-3	Ensure at least the current and previous router configurations are stored in a secured location to ensure a proper recovery path.	1. Cisco – Have the router administrator show the stored configuration files.	Current and previous configurations exist and are stored in a secured location for recovery.			

Test ID	**NIST ID**	Test Objective	Test Steps	Expected Results	Actual Results	Pass / Fail	**Comments/Supporting Evidence**
40	AU-4, AC-3	Ensure the system where router configuration files are stored uses local operating system's security mechanisms for restricting access to the files (i.e., password restricted file access). Ensure only authorized router administrators are given access to the stored configuration files.	1. Have the router administrator display the security features that are used to control access to the configuration files. 2. Interview the ISSO to ensure access to stored configuration files is restricted to authorized router administrators only.	Router configurations are securely stored on a local machine.			
41	IA-7	Ensure that unencrypted router passwords are not stored in an offline configuration file.	1. Review the stored router configuration files to ensure passwords are not stored in plain-text format.	Unencrypted passwords are not stored in an offline configuration file.			
42	AC-3	Ensure that all Trivial File Transfer Protocol (TFTP) implementations are authorized and have maintained justification.	1. Verify written authorization is with the ISSO. 2. Interview the router administrator to see how they transfer the router configuration files to and from the router. Verify the running configuration for all Cisco routers have statements similar to the following: ip ftp username xxxx ip ftp password 7 xxxx	TFTP implementations are authorized and have maintained justification.			

Test ID	**NIST ID**	Test Objective	Test Steps	Expected Results	Actual Results	Pass / Fail	**Comments/Supporting Evidence**
43	AC-3, IA-3	If Trivial File Transfer Protocol (TFTP) implementation is used, ensure the TFTP server resides on a controlled managed Local Area Network (LAN) subnet, and access is restricted to authorized devices within the local enclave.	1. Identify TFTP server addresses and determine if LAN has traffic restrictions and devices with access to server have Access Control List (ACL) permissions and restrictions.	Ensure Trivial File Transfer Protocol (TFTP) implementations reside on a controlled managed LAN subnet and access is restricted to authorized devices within the local enclave.			
44	IA-2	Ensure the File Transfer Protocol (FTP) username and password are configured.	1. Review the running configuration for all routers to ensure a username and password have been configured for the router's ftp client. The configuration should look similar to the following: ip ftp username userid ip ftp password psw	FTP username and password are configured.			

Test ID	**NIST ID**	Test Objective	Test Steps	Expected Results	Actual Results	Pass / Fail	**Comments/Supporting Evidence**
45	AU-7	Checks to see if sufficient security relevant data is captured in system logs.	Procedures: 1. From an enable console window, type 'sh run | inc service timestamps log'. Response should read: 2. Review the logging mechanism to see what elements are recorded. (If syslog servers are being used, you can use the command "show logging" to see the setup.) The following elements are selected to be recorded in the log: Expected Results: 1. "service timestamps log datetime". 2. - User ID (if available), but do not log password used; - Action/request attempted (particularly: interface status changes, changes to the system configuration, access list matches and/or failures) - Success or failure of the action; - Date/time stamp of the event and Source address of the request. 3. If the router is configured for dial-up access, confirm that logging provides explicit audit trails for all dial-up access. Note that it is OK for this line to have additional arguments, as long as it contains these four words.	Checks to see if sufficient security relevant data is captured in system logs.			

Test ID	**NIST ID**	Test Objective	Test Steps	Expected Results	Actual Results	Pass / Fail	**Comments/Supporting Evidence**
46	AC-13, AU-6, AU-9, AU-11	Checks to see if the organization supervises and reviews the activities of users with respect to the enforcement and usage of information system access controls. Checks to see that audit logs are retained for the required amount of time and are protected from tampering or deletion.	Procedures: 1. Verify that logs are reviewed and analyzed on a periodic basis, and that the results of each review are documented and given to management. 2. Verify that security-related events are recorded in the logs and are available to Security and Telecomm Management staff members. This must include unsuccessful attempts to access routers (ACL violations and logon failures) 3. Verify that gaps in log data are treated as a possible sign of logging being disabled. Steps need to be taken to ensure that logging is enabled and functioning properly. 4. Verify that logging is configured such that all audit disabling or failures are recorded. 5. Verify that audit log data is protected from deletion or modification	The organization supervises and reviews the activities of users with respect to the enforcement and usage of information system access controls.			

Test ID	**NIST ID**	Test Objective	Test Steps	Expected Results	Actual Results	Pass / Fail	**Comments/Supporting Evidence**
47	CM-3, CM-4, CM-6, SI-2	Ensure all router changes and updates are documented in a manner suitable for review. Ensure request forms are used to aid in recording the audit trail of router change requests. Ensure changes and modifications to routers are audited so they can be reviewed. Ensure current paper or electronic copies of router configurations are maintained in a secure location. Ensure only authorized personnel, with proper verifiable credentials, are allowed to request changes to routing tables or service parameters.	1. Have the ISSO provide copies of router change request forms for visual inspection. 2. Have the ISSO provide copies of router change request forms for visual inspection. 3. Interview ISSO and router administrator to verify compliance.	Configuration management procedures are in place.			
48	AU-4	Ensure that the log server has the capacity to retain the logs for the required retention period.	Examine the available storage capacity of the log server.	The log server has enough disk space to retain the logs for the required retention period.			

IRS Safeguard SCSEM Legend

Test Case Tab: Execute the test cases and document the results to complete the IRS Safeguard Computer Security review. Reviewer is required to complete the following columns: Actual Results, Comments/Supporting Evidence. Please find more details of each column below.

Test ID	Identification number of SCSEM test case
NIST ID	NIST 800-53/PUB 1075 Control Identifier
Test Objective	Objective of test procedure.
Test Steps	Detailed test procedures to follow for test execution.
Expected Results	The expected outcome of the test step execution that would result in a Pass.
Actual Results	The actual outcome of the test step execution, i.e., the actual configuration setting observed.
Pass/Fail	Reviewer to indicate if the test case pass, failed or is not applicable.
Comments / Supporting Evidence	Reviewer to include any supporting evidence to confirm if the test case passed., failed on not applicable As evidence, provide the following information for the following assessment methods: 1. Interview - Name and title of the person providing information. Also provide the date when the information is provided. 2. Examination - Provide the name, title, and date of the document referenced as the evidence. Also provide section number where the pertinent information is resident within the document (if possible). Ensure all supporting evidence to verify the test case passed or failed. If the control is marked as NA, then provide appropriate justification as to why the control is considered NA.

Version	Release Date	Summary of Changes	Name
0.1	12/7/2007	First Release	Jonathan Isner
0.2	4/16/2008	Updated warning banner language based on the IRS.gov warning banner.	Jonathan Isner
0.3	7/2/2008	Updated the NIST IDs for Test Router-47 to include CM-3, CM-4, CM-6, SI-2.	Jonathan Isner
0.4	10/9/2008	Split test case 40 into two test cases - #48 is the new test case.	
0.5	12/3/2008	Added command to test ID 32 and 33.	Jonathan Isner